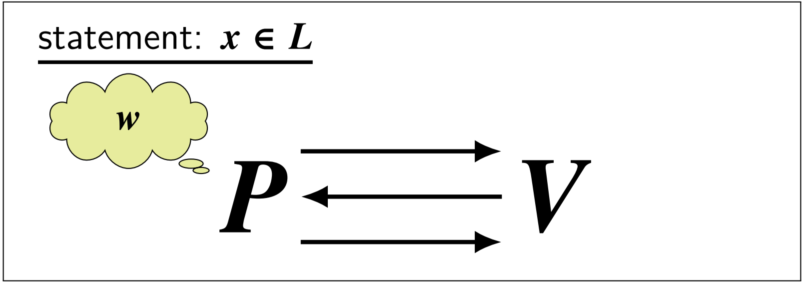
Resettable Statistical Zero-Knowledge for NP

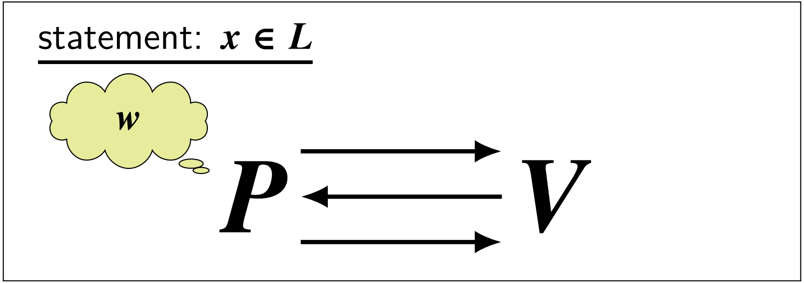
Susumu Kiyoshima*

*Today is my birthday! Yay

Zero-knowledge (ZK) arguments



Zero-knowledge (ZK) arguments

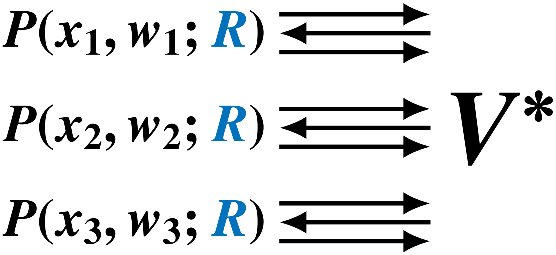


- **Completeness**: When $x \in L$, honest P can convince V
- **Soundness**: When $x \notin L$, any PPT P^* cannot convince V
- **ZK**: When $x \in L$, any PPT V^* cannot learn anything beyond $x \in L$

Resettable ZK

- ZK in setting where P generates many proofs using same randomness

  [Canetti, Goldreich, Goldwasser, Micali. 2000]

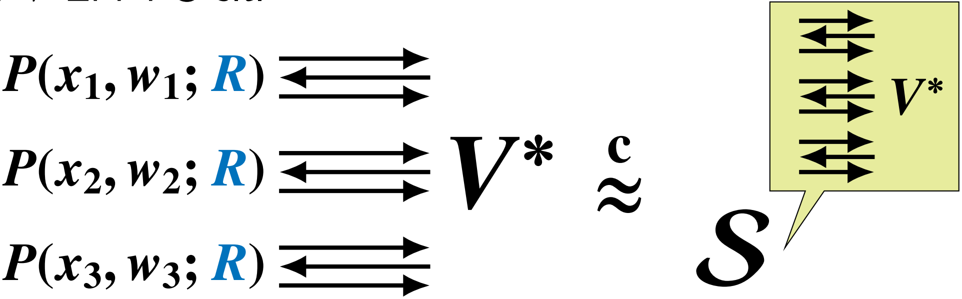


Resettable ZK

- ZK in setting where P generates many proofs using same randomness

  [Canetti, Goldreich, Goldwasser, Micali. 2000]

$\forall$PPT $V^* \exists$PPT $\mathcal{S}$ s.t.



Why study resettable ZK?

- **Theoretical motivation:**
  - **Understanding the role of randomness**

    ($\boldsymbol{P}$ doesn't need to sample fresh randomness in each proof)
- **Practical motivation:**
  - **Minimizing cost of randomness generation**

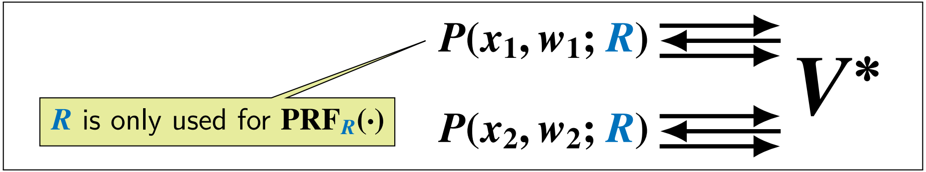
    (Let's sample randomness once and reuse it subsequently!)
  - **Preventing physical resetting attacks**

    (ZK holds even when $\boldsymbol{V}^*$ "unplugs" $\boldsymbol{P}$ to force $\boldsymbol{P}$ to reuse same randomness!)

Known results on resettable ZK

- **Strong positive results are known** 😄
  - E.g., construction from one-way functions in the plain model [Chung, Pass, Seth. 2013]

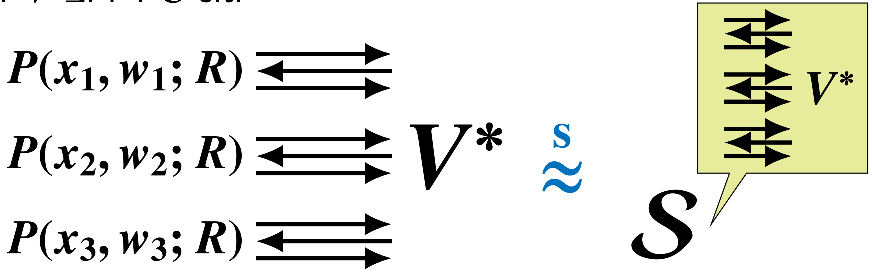
- **High-level idea:**
  - Different proofs are generated with "computationally independent" pseudorandomness (all sampled with common PRF key $\boldsymbol{R}$)



Resettable ZK + Statistical ZK?

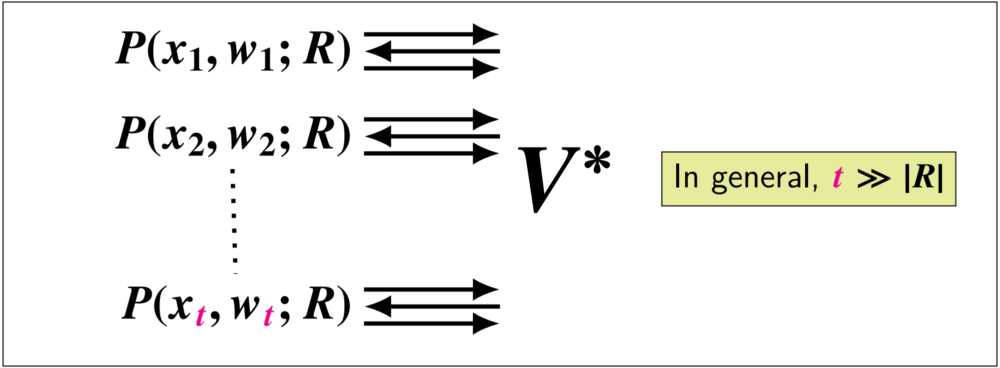
- **Resettable statistical ZK (Resettable SZK)**:
  SZK in setting where many proofs are generated using the same prover randomness [Garg, Ostrovsky, Visconti, Wadia. 2012]

$\forall$PPT $V^* \exists$PPT $\mathcal{S}$ s.t.



Resettable SZK is hard to obtain 😣

- **Difficulty**: We need to achieve SZK in unbounded-poly number of proofs using fixed-length prover randomness
  - Pseudorandomness does not seem helpful to overcome this difficulty



Known result on resettable SZK

- Resettable SZK proof exists for any language L that admits hash proof systems [Garg, Ostrovsky, Visconti, Wadia. 2012] 😄
  - More precisely requirement for L is to have appropriate instance-dependent commitments

Known result on resettable SZK

- Resettable SZK proof exists for any language L that admits hash proof systems [Garg, Ostrovsky, Visconti, Wadia. 2012] 😄
  - More precisely requirement for L is to have appropriate instance-dependent commitments

Our target: Resettable SZK argument for NP

Our Result

Our Result

NTT

Assuming the existence of one-way functions (OWFs),
resettable SZK argument for NP $\Longleftrightarrow$ witness encryption for NP

Our Result

Assuming the existence of one-way functions (OWFs), resettable SZK argument for NP $\iff$ witness encryption for NP

- **Witness encryption (WE)** [Garg, Gentry, Sahai, Waters. 2013]:
  - A generalization of public-key encryption, where $\mathbf{pk}$ is an NP instance $x \in L$ and $\mathbf{sk}$ is any corresponding witness w. (Semantic security holds when $x \notin L$)

Our Result

Assuming the existence of one-way functions (OWFs), resettable SZK argument for NP $\Longleftrightarrow$ witness encryption for NP

- **Theorem 1 (WE $\Rightarrow$ Resettable SZK):** Assume OWF and WE for NP language L. Then, there exists resettable SZK argument for L.
  - Easy (folklore)
- **Theorem 2 (Resettable SWI $\Rightarrow$ WE):** Assume OWF and resettable statistical witness-indistinguishable (resettable SWI) argument for NP. Then, there exists WE for NP.
  - Difficult (main technical contribution)

How to interpret our result

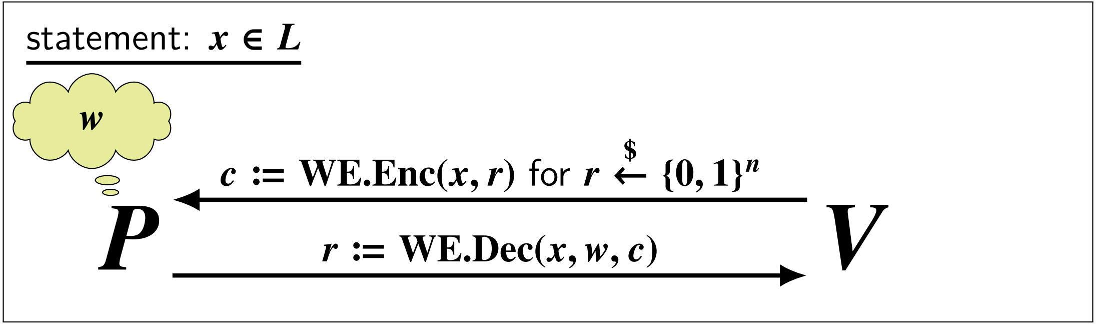
- **If you are pessimist:** negative result for resettable SZK 😫
  - Constructing resettable SWI/SZK for NP is as hard as constructing WE for NP
- **If you are optimist:** yet another reason to study WE 😁
  - The only way to improve state-of-the-art of resettable SZK (efficiency, assumption, etc.) is to improve state-of-the-art of WE

Our Techniques, part 1

(WE for $\boldsymbol{L} \Longrightarrow$ Resettable SZK for $\boldsymbol{L}$)

Protocol description

- **Simple case:** Resettable SWI against honest V



Protocol description

- **Simple case:** Resettable SWI against honest V

statement: $x \in L$

Key Point for resettable SWI:

Transcript is independent of w

w

$$c := \mathrm{WE.Enc}(x, r) \text{ for } r \xleftarrow{\$} \{0,1\}^n$$

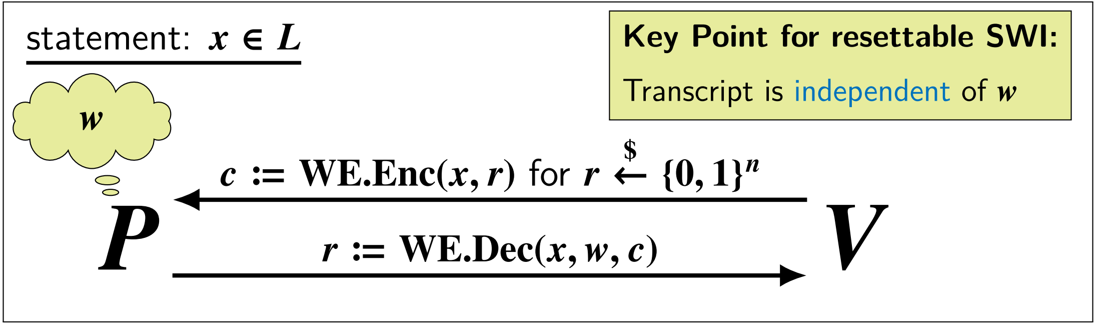
$P \leftarrow V$

$$r := \mathrm{WE.Dec}(x, w, c)$$

$P \rightarrow V$

Protocol description

- **Simple case:** Resettable SWI against honest V



- Full-fledged resettable SZK is obtained via known transformation (enabling simulator to obtain trapdoor) [Garg, Ostrovsky, Visconti, Wadia. 2012]

Our Techniques, part 2

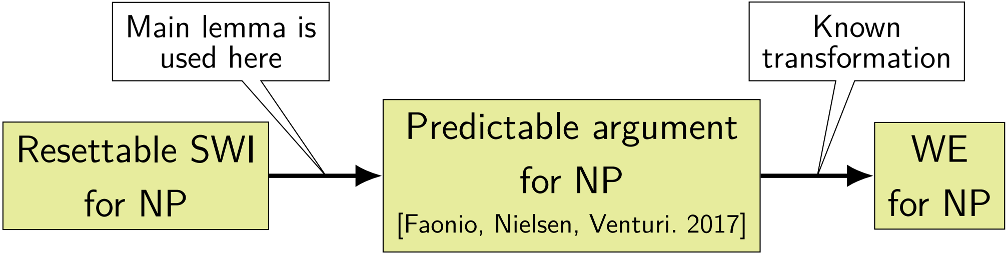
(Resettable SWI for NP $\Longrightarrow$ WE for NP)

Overall approach

- **Main lemma: “Witness-independent transcript” is necessary for resettable SWI**
  - I.e., $P(x, w_0; R)$ and $P(x, w_1; R)$ generate identical transcript w.h.p.
    (This is much stronger than normal SWI)

Overall approach

- **Main lemma:** **"Witness-independent transcript" is necessary for resettable SWI**
  - I.e., $P(x, w_0; R)$ and $P(x, w_1; R)$ generate identical transcript w.h.p. (This is much stronger than normal SWI)



Predictable argument (PA)

PA = Interactive argument where V can predict prover messages using its secret coin [Faonio, Nielsen, Venturi. 2017]

- **Example:** Interactive proof for graph non-isomorphism [Goldreich, Micali, Wigderson. 1991]
  - Given (G_0, G_1), V picks $b \in \{0, 1\}$, sends random graph isomorphic to G_b, and checks whether P replies with b

Predictable argument (PA)

PA = Interactive argument where V can predict prover messages using its secret coin [Faonio, Nielsen, Venturi. 2017]

- **Example:** Interactive proof for graph non-isomorphism [Goldreich, Micali, Wigderson. 1991]
  - Given (G_0, G_1), V picks $b \in \{0, 1\}$, sends random graph isomorphic to G_b, and checks whether P replies with b
- **Security:** Completeness and soundness
- **Known result:** PA for $L \iff$ WE for L [Faonio, Nielsen, Venturi. 2017]

Resettable SWI for NP $\Longrightarrow$ PA for NP

Resettable SWI for NP $\Longrightarrow$ PA for NP

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$

Resettable SWI for NP $\Longrightarrow$ PA for NP

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$

$P(x, w)$ $V(x)$

Resettable SWI for NP $\Longrightarrow$ PA for NP

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$

$P(x, w)$

$V(x)$

In V's head:
1. Sample $\hat{x} \in \hat{L}$ by $\hat{x} := (x, \mathbf{PRG}(s))$ for $s \xleftarrow{\$} \{0,1\}^n$
2. Run $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ with statement $\hat{x}$, witness s, and prover randomness $R \xleftarrow{\$} \{0,1\}^*$
3. Let $(v_1, p_1, \ldots, v_\rho, p_\rho)$ be the resulting transcript

Resettable SWI for NP $\Longrightarrow$ PA for NP

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$

In V's head:

1. Sample $\hat{x} \in \hat{L}$ by $\hat{x} := (x, \mathbf{PRG}(s))$ for $s \xleftarrow{\$} \{0,1\}^n$
2. Run $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ with statement $\hat{x}$, witness s, and prover randomness $R \xleftarrow{\$} \{0,1\}^*$
3. Let $(v_1, p_1, \ldots, v_\rho, p_\rho)$ be the resulting transcript

Resettable SWI for NP $\Longrightarrow$ PA for NP

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$

$P(x, w)$ $\qquad\qquad$ $V(x)$

$\longleftarrow$ $\hat{x}, R, v_1$

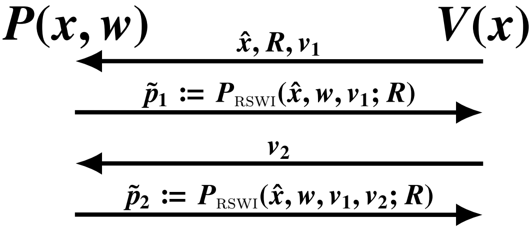
$\tilde{p}_1 := P_{\mathrm{RSWI}}(\hat{x}, w, v_1; R)$ $\longrightarrow$

In V's head:

1. Sample $\hat{x} \in \hat{L}$ by $\hat{x} := (x, \mathbf{PRG}(s))$ for $s \xleftarrow{\$} \{0,1\}^n$
2. Run $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ with statement $\hat{x}$, witness s, and prover randomness $R \xleftarrow{\$} \{0,1\}^*$
3. Let $(v_1, p_1, \ldots, v_\rho, p_\rho)$ be the resulting transcript

Resettable SWI for NP $\Longrightarrow$ PA for NP

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$

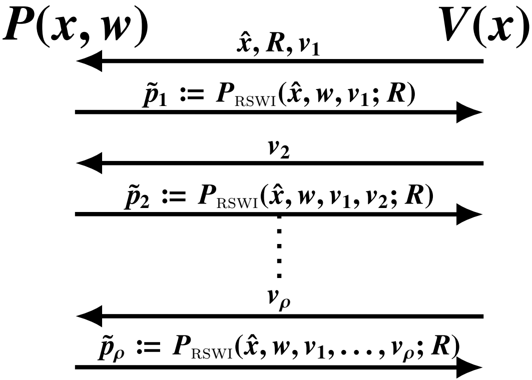


In V's head:

1. Sample $\hat{x} \in \hat{L}$ by $\hat{x} := (x, \mathbf{PRG}(s))$ for $s \xleftarrow{\$} \{0,1\}^n$
2. Run $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ with statement $\hat{x}$, witness s, and prover randomness $R \xleftarrow{\$} \{0,1\}^*$
3. Let $(v_1, p_1, \ldots, v_\rho, p_\rho)$ be the resulting transcript

Resettable SWI for NP $\Longrightarrow$ PA for NP

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$

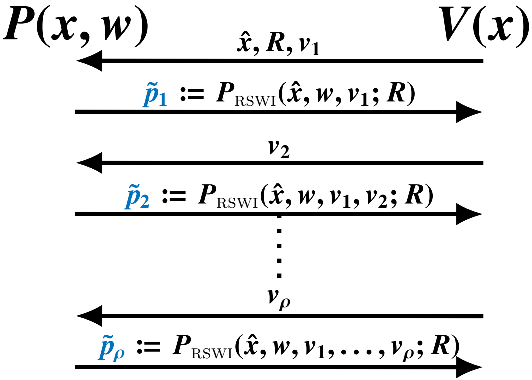


In V's head:

1. Sample $\hat{x} \in \hat{L}$ by $\hat{x} := (x, \mathbf{PRG}(s))$ for $s \xleftarrow{\$} \{0,1\}^n$
2. Run $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ with statement $\hat{x}$, witness s, and prover randomness $R \xleftarrow{\$} \{0,1\}^*$
3. Let $(v_1, p_1, \ldots, v_\rho, p_\rho)$ be the resulting transcript

Resettable SWI for NP $\Longrightarrow$ PA for NP

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$



In V's head:

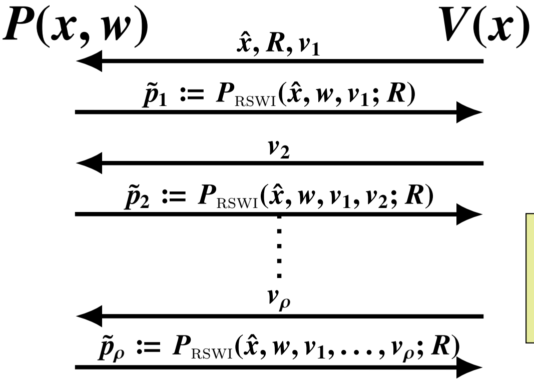
1. Sample $\hat{x} \in \hat{L}$ by $\hat{x} := (x, \mathbf{PRG}(s))$ for $s \xleftarrow{\$} \{0,1\}^n$
2. Run $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ with statement $\hat{x}$, witness s, and prover randomness $R \xleftarrow{\$} \{0,1\}^*$
3. Let $(v_1, p_1, \ldots, v_\rho, p_\rho)$ be the resulting transcript

Accept iff $p_i = \tilde{p}_i$ for all i

Resettable SWI for NP $\Longrightarrow$ PA for NP

NTT

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$



In V's head:

1. Sample $\hat{x} \in \hat{L}$ by $\hat{x} := (x, \mathbf{PRG}(s))$ for $s \xleftarrow{\$} \{0, 1\}^n$
2. Run $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ with statement $\hat{x}$, witness s, and prover randomness $R \xleftarrow{\$} \{0, 1\}^*$
3. Let $(v_1, p_1, \ldots, v_\rho, p_\rho)$ be the resulting transcript

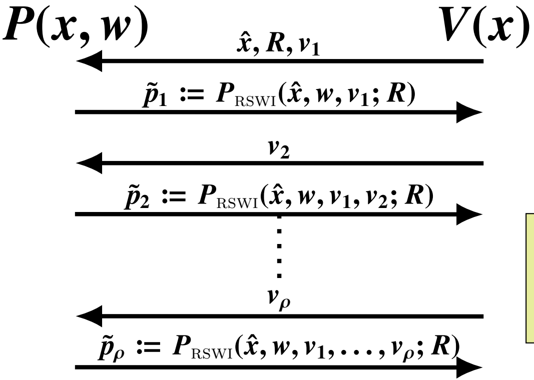
predictability & soundness: ✔

Accept iff $p_i = \tilde{p}_i$ for all i

Resettable SWI for NP $\Longrightarrow$ PA for NP

NTT

- **Approach:** Constructing PA for L using resettable SWI argument $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ for related language $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathbf{PRG}(s)\}$



In V's head:

1. Sample $\hat{x} \in \hat{L}$ by $\hat{x} := (x, \mathbf{PRG}(s))$ for $s \xleftarrow{\$} \{0,1\}^n$
2. Run $(P_{\mathrm{RSWI}}, V_{\mathrm{RSWI}})$ with statement $\hat{x}$, witness s, and prover randomness $R \xleftarrow{\$} \{0,1\}^*$
3. Let $(v_1, p_1, \ldots, v_\rho, p_\rho)$ be the resulting transcript

predictability & soundness: ✔

completeness: ✔ (from Main Lemma, guaranteeing witness-independent transcript)

Accept iff $p_i = \tilde{p}_i$ for all i

How is Main Lemma proven?

How is Main Lemma proven?

NTT

See the paper!

Hint: If $\neg$(witness-independent transcript), we can break resettable SWI by comparing:

- **Exp 1:** For each $i = 1, \ldots, t$, run $P_{\text{RSWI}}((x, \mathrm{PRG}(s_i)), w; R)$ with common R
- **Exp 2:** For each $i = 1, \ldots, t$, run $P_{\text{RSWI}}((x, \mathrm{PRG}(s_i)), w; R)$ or $P_{\text{RSWI}}((x, \mathrm{PRG}(s_i)), s_i; R)$ with common R

Conclusion

Conclusion

Our Result:

- **Theorem 1 (WE ⇒ Resettable SZK):** Assume OWF and WE for NP language L. Then, there exists resettable SZK argument for L.
  - Easy (folklore)

- **Theorem 2 (Resettable SWI ⇒ WE):** Assume OWF and resettable SWI argument for NP. Then, there exists WE for NP.
  - Difficult (main technical contribution)

Conclusion

Our Result:

- **Theorem 1 (WE ⇒ Resettable SZK):** Assume OWF and WE for NP language L. Then, there exists resettable SZK argument for L.
  - Easy (folklore)
- **Theorem 2 (Resettable SWI ⇒ WE):** Assume OWF and resettable SWI argument for NP. Then, there exists WE for NP.
  - Difficult (main technical contribution)

Thanks!

Appendix

Resettable SWI $\Rightarrow$ Witness-independent transcript

$\neg$ Witness-independent transcript $\Rightarrow$ $\neg$ Resettable SWI

¬ Witness-independent transcript ⇒ ¬ Resettable SWI

Toy example (We assume ¬ Witness-independent transcript for all statements & randomness)

- Suppose $P(\hat{x}_i, w_i; R)$ and $P(\hat{x}_i, s_i; R)$ generate different transcripts for $\forall \hat{x}_1, \ldots, \hat{x}_t \in \hat{L}$
  (Recall: $\hat{L} := \{(x, r) \mid x \in L$ OR $\exists s$ s.t. $r = \mathbf{PRG}(s)\}$)

¬ Witness-independent transcript ⇒ ¬ Resettable SWI

Toy example (We assume ¬ Witness-independent transcript for all statements & randomness)

- Suppose $P(\hat{x}_i, w_i; R)$ and $P(\hat{x}_i, s_i; R)$ generate different transcripts for $\forall \hat{x}_1, \ldots, \hat{x}_t \in \hat{L}$
  (Recall: $\hat{L} := \{(x, r) \mid x \in L$ OR $\exists s$ s.t. $r = \mathbf{PRG}(s)\}$)

Exp1:

Exp2:

¬ Witness-independent transcript ⇒ ¬ Resettable SWI

NTT

Toy example (We assume ¬ Witness-independent transcript for all statements & randomness)

- Suppose $P(\hat{x}_i, w_i; R)$ and $P(\hat{x}_i, s_i; R)$ generate different transcripts for $\forall \hat{x}_1, \ldots, \hat{x}_t \in \hat{L}$

  (Recall: $\hat{L} := \{(x, r) \mid x \in L$ OR $\exists s$ s.t. $r = \mathbf{PRG}(s)\}$)

Exp1: (for each i, w_i is used)

$P(\hat{x}_1, w_1; R)$ proof →

⋮

$P(\hat{x}_t, w_t; R)$ proof →

V^*

Exp2:

¬ Witness-independent transcript ⇒ ¬ Resettable SWI

NTT

Toy example (We assume ¬ Witness-independent transcript for all statements & randomness)

- Suppose $P(\hat{x}_i, w_i; R)$ and $P(\hat{x}_i, s_i; R)$ generate different transcripts for $\forall \hat{x}_1, \ldots, \hat{x}_t \in \hat{L}$

  (Recall: $\hat{L} := \{(x, r) \mid x \in L$ OR $\exists s$ s.t. $r = \mathbf{PRG}(s)\}$)

Exp1: (for each i, w_i is used)

$P(\hat{x}_1, w_1; R)$ proof → V^*

⋮

$P(\hat{x}_t, w_t; R)$ proof → V^*

Exp2: (for each i, w_i or s_i is chosen randomly)

$P(\hat{x}_1, w_1; R)$ or $P(\hat{x}_1, s_1; R)$ proof → V^*

⋮

$P(\hat{x}_t, w_t; R)$ or $P(\hat{x}_t, s_t; R)$ proof → V^*

¬ Witness-independent transcript ⇒ ¬ Resettable SWI

Toy example (We assume ¬ Witness-independent transcript for all statements & randomness)

- Suppose $P(\hat{x}_i, w_i; R)$ and $P(\hat{x}_i, s_i; R)$ generate different transcripts for $\forall \hat{x}_1, \ldots, \hat{x}_t \in \hat{L}$

  (Recall: $\hat{L} := \{(x, r) \mid x \in L$ OR $\exists s$ s.t. $r = \mathrm{PRG}(s)\}$)

Exp1: (for each i, w_i is used)

$P(\hat{x}_1, w_1; R)$ proof

⋮

$P(\hat{x}_t, w_t; R)$ proof

V^*

#(transcripts) $\leq 2^{|R|}$

Exp2: (for each i, w_i or s_i is chosen randomly)

$P(\hat{x}_1, w_1; R)$ or $P(\hat{x}_1, s_1; R)$ proof

⋮

$P(\hat{x}_t, w_t; R)$ or $P(\hat{x}_t, s_t; R)$ proof

V^*

¬ Witness-independent transcript ⇒ ¬ Resettable SWI

Toy example (We assume ¬ Witness-independent transcript for all statements & randomness)

- Suppose $P(\hat{x}_i, w_i; R)$ and $P(\hat{x}_i, s_i; R)$ generate different transcripts for $\forall \hat{x}_1, \ldots, \hat{x}_t \in \hat{L}$
  (Recall: $\hat{L} := \{(x, r) \mid x \in L \text{ OR } \exists s \text{ s.t. } r = \mathrm{PRG}(s)\}$)

Exp1: (for each i, w_i is used)

$P(\hat{x}_1, w_1; R)$ proof

⋮

$P(\hat{x}_t, w_t; R)$ proof

V^*

#(transcripts) $\leq 2^{|R|}$

Exp2: (for each i, w_i or s_i is chosen randomly)

$P(\hat{x}_1, w_1; R)$ or $P(\hat{x}_1, s_1; R)$ proof

⋮

$P(\hat{x}_t, w_t; R)$ or $P(\hat{x}_t, s_t; R)$ proof

V^*

#(transcripts) $\geq 2^t$

¬ Witness-independent transcript ⇒ ¬ Resettable SWI

Toy example (We assume ¬ Witness-independent transcript for all statements & randomness)

- Suppose $P(\hat{x}_i, w_i; R)$ and $P(\hat{x}_i, s_i; R)$ generate different transcripts for $\forall \hat{x}_1, \ldots, \hat{x}_t \in \hat{L}$
  (Recall: $\hat{L} := \{(x, r) \mid x \in L$ OR $\exists s$ s.t. $r = \mathbf{PRG}(s)\}$)

Exp1: (for each i, w_i is used)

$P(\hat{x}_1, w_1; R)$ → proof

⋮

$P(\hat{x}_t, w_t; R)$ → proof

V^*

#(transcripts) $\leq 2^{|R|}$

Exp2: (for each i, w_i or s_i is chosen randomly)

$P(\hat{x}_1, w_1; R)$ or $P(\hat{x}_1, s_1; R)$ → proof

⋮

$P(\hat{x}_t, w_t; R)$ or $P(\hat{x}_t, s_t; R)$ → proof

V^*

#(transcripts) $\geq 2^t$

When $t \gg |R|$, we have Exp1 $\not\approx$ Exp2